Qualys WAS 4.8 New Features

We are pleased to announce Qualys Web Application Scanning 4.8 (WAS) featuring quick and easy vulnerability retest functionality, without having to launch a full scan as well as the ability to customize the severity of findings to meet your business needs.

Feature Highlights:

- Vulnerability Retest Functionality
- Vulnerability Severity Customization for Findings

Other Features and Changes:

- Enhanced Display for Severity Level Text with Severity Icon
- Enhanced Reporting Detail for Function
- WAS Module Global Settings Support

Vulnerability Retest Functionality

Customers can now quickly retest vulnerability findings individually in WAS without launching another full scan. Within the Detections Tab, "Retest" will launch a scan to test the selected finding. Only potential vulnerabilities, confirmed vulnerabilities and sensitive contents are available for retest.

V	New	150124	Clickjacking - Framable Page	Quick Actions	May 2016	0	
	http://funky	town.vuln	.qa.qualys.com/cassium/	View			
	New	150085	Slow HTTP POST vulnerability	Ignore Activate	May 2016	6	
	http://10.10	.26.238/		Piotivulo			
	New	150079	Slow HTTP headers vulnerability	Install Patch Remove Patch	May 2016	6	
	- http://10.10	150067	Links Discovered During User-Agent and Mobile Site Checks	Retest Cancel Retest	May 2016	6	

This will show a confirmation message for the retest action.

Confirm Finding!	×
Are you sure you want to confirm the selected findings	
Scanner will re test selected finding and it will update status accordingly	
Cancel	Confirm

Users can also cancel the retest.

☑ Retesting 150060 HTTP Response Splitting Vulnerabilities	Quick Actions	May 2016	6	
https://10.10.26.238/boq/parseAction.php	View			
New 150049 Login Brute Force Vulnerability	Ignore	May 2016	6	
https://10.10.26.238/boq/parseAction.php	Activate			
New 150124 Clickjacking - Framable Page	Install Patch	May 2016	0	
http://funkytown.vuln.qa.qualys.com/cassium/	Remove Patch			
New 150085 Slow HTTP POST vulnerability	Cancel Retest	May 2016	6	
http://10.10.26.238/				
			~	

This will show a confirmation message to cancel the retest action.

Cancel Retest	×
Are you sure you wants to cancel retesting?	
Note that cancel option is handled by scanner, Retesting may have already completed	
Cancel	Confirm

Once a user launches the retest, and when finding is still under the test phase, the view panel will be updated as follows. There is also a cancel link on top of the right side so a user can click this link to cancel the retesting if desired.

ulnerability	/ Details				
I This fi	inding is cu	rrently being retested			Cancel
Reques Applian Date	sted by: ice	Snehal Mandavkar (quays External 07 May 2016 5:41PM GMT	s_sm) ⊊+0530		
This p	anel will be re	freshed as soon as the chec	k completes. Please wait for a moment.		
RL: https://10.	10.26.238/bog	/parseAction.php	ves Web Application	Test App <iframe></iframe>	Activ
atch #	- Information	Disclosure	Authentication	Not Used	
ie ap	CWE-113		First Time Detected	04 May 2016 2:40PM GMT+0530 04 May 2016 2:40PM GMT+0530	
WE WASP ASC	A5 Security WASC-24 H	Misconfiguration TTP Request Splitting	Last Time Detected	04 May 2016 2:40PM GMT+0530	
WE WASP ASC VSS Base	A5 Security WASC-24 H 7.5	Misconfiguration TTP Request Splitting CVSS Temporal 6.7	Last Time Detected Last Scan Date Times Detected	04 May 2016 2:40PM GMT+0530 1 View History	
WE WASP ASC VSS Base Details	A5 Security WA SC-24 H 7.5	Misconfiguration TTP Request Splitting CVSS Temporal 6.7	Last Time Detected Last Scan Date Times Detected	04 May 2016 2:40PM GMT+0530 1 View History	Show
WE WASP VSS Base Details	A5 Security WA SC-24 H 7.5	Misconfiguration TTP Request Splitting CVSS Temporal 6.7	Last Time Detected Last Scan Date Times Detected	04 May 2016 2:40PM GMT+0530 1 View History	Show
WE WASP ASC VSS Base Details Detection	A5 Security WA SC-24 H 7.5 Information It ha: The	Misconfiguration TTP Request Splitting CVSS Temporal 6.7 been detected by exploiting bayloads section will display a	Last Time Detected Last Scan Date Times Detected the parameter login of the form located i a list of tests that show how the param cou	04 May 2016 2:40PM GMT+0530 1 View History n URL http://10.10.26.238/ ild have been exploited to collect the information	Show

Once the retest is finished the view dialog will be updated as follows:

Case 1: When Finding is fixed in retest. Status changed to Fixed.	Case 2: Finding is detected in retest. Status changed to Active.							
Vulnerability Details	Vulnerability Details							
Requested by: Snehal Mandavkar (quays_sm) Appliance: External Date: 06 May 2016 11:34PM GMT+0530 Status: Finding has not been detected Reason: Vulnerable URL cannot not be found anymore	This finding is retested Requested by: Snehal Mandavkar (quays_sm) Appliance: External Date: 07 May 2016 3:51PM GMT+0530 Status: Finding has been detected Reason: Finding could have been confirmed							
URL: https://10.10.26.238/bog/parseAction.php	URL: http://10.10.26.238/							

Vulnerability Severity Customization for Findings

Users will now have the ability to customize the vulnerability severity of findings within Detections. This ability now pertains to vulnerability and sensitive content findings reported in their web applications. In addition, users will be able to specify comments along with any change made. Also, action logs shall be created to track changes made on the severity level. Visibility is available to show what was the Qualys severity level was prior to being updated. The severity level change shall have an impact on the dashboard stats, web application reports and when viewing detections.

Each detection that had the severity level altered will use a different severity icon than standard:

- The customized severity level will be displayed
- The Qualys standard level will be visible by using a small arrow to show which level the new value has been set from.

Increased severity examples

Decreased severity examples

Dashboard Web Applic	ations Scans	Burp	Reports	Configuration	KnowledgeBase								
Web Application	Management	Web Ap	plications	Authentication	Detections	Catalog	Maps						
earch Results	Actions (1) 💙				_					4 1-4	of 4	₽	æ 🐡 🗸
Search	Status QID	Name						 Group 	Last Detected	Age	Patch	Severity	
Filter Results Target	Fixed 2700 http://10.10.26.23	1 FTP user 8:80/	s with Blank P	assword Allowed				-	20 Nov 2009	2359			Confirmed Vulnera
b Application	Fixed 1500 http://10.10.26.23	04 Path-Bas 8:80/bog/prote	ed Vulnerability cted/mime/def	aultPage.tsp.bak				-	20 Nov 2009	2359			Qualys standard le
	New 2060 http://lamp.vuln.q-	15 Web Serv a.qualys.com:8	ver Not Found 30/cassium/ser	isilive_content/combo.ht	tml			-	18 Jan 2010	2299			
↓ Ja	Fixed 2700 http://10.10.26.23	2 Writeable 8:80/bog/prote	Root Directory	on FTP Server aultPage.tsp.bak				-	20 Nov 2009	2359			
at Scan Date													

By moving the mouse over the icon, the user will also know what the Qualys standard level was prior to the change.

Qualys standard level - <severity level>

The same icon with tooltip will be available in the preview panel.

Edit Severity Dialog:

With this action, a dialog will open allowing the user to change the severity level on one or more findings. A mandatory comment is required by the user.

Edit Severity Level						×				
You are about to change the severity of this vulnerability.										
Severity level for this findings is 4. The severity will be updated for only this instance, not all instances of this QID. Comment will be available when viewing finding from reports.										
Move the slider to set new level for	vulnerability.									
Custom Level	1	2	3	4	5					
				_	Qualys st	andard level				
Comment*										
seventy edited to 4										
Cancel						Save				
:38/bog/parseAction.php : Copy of Vuln Retest WebApp (Deleted Sc	an) , Vulnerable P	arameter: qu	estion_box, S	Status: New						
07				First D	latantari	Last Natastari				

The severity level change shall have an impact on the entire WAS module, including dashboard stats, web application reports and when viewing detections.

Dashboard						
Mon 09 May 2016 3 total scanned web apps 0 with Malware Monitoring	All Vulnerabilities	HIGH Severity 1	MED Severity 0	LOW Severity 2	Malware SAFE 0 detections	New Scan Y Add Web Application
MOST VULNERABLE WEB APPLICATIONS				View All	🗘 CATALOG	v
b Application Name	Last Scan Date	Total Vulnerabilities	High Med Lov	v Severity	No rec	ords.
11 VR-5 Apple ation 3/110 10 28 238 80/	28 Apr 2016	3	1 – 2	HIGH		
		Dashl	ooard stats			
Auharshilitia ku Group		OWA SP Top 10 2013	Welnershilities			
unicabilities by Gloup		Injection	vumerabilities			
		Broken Authenti	cation and Session Ma	nagement		
		Insecure Direct (ung (XSS) Object References			
		Security Misconf	iguration			
		Sensitive Data E	cposure Level Access Control			
		Cross-Site Requ	est Forgery (CSRF)			
Cross-Site SQL Path Scripting Injection Disclosure	Information Disclosure	Using Componen Unvalidated Red	its with Known Vulner.	ibilities		
	Level 5 Level 4	Level 3 Lev	el 2 Level 1	Sensitive Conte	ents Informatio	n Gathered
b Application	0 0	0 0	0 0	1		D
tb Application						
b Application (WA.S Application esuits (1)						
b Application (WA S Application esuits (1) esuits (1)						

Restore Severity Level Dialog:

With this action, a dialog will open allowing a user to restore the default severity level set by Qualys on all selected findings. A confirmation dialog will be displayed, explaining to the user the impact of the change.

Customize Detections	×
A You are about to reset the severity level to one or more detections	(*) REQUIRED FIELDS
The findings will be applied back the severity level defined by Qualys. The security risk of the assoc application(s) will be recomputed and be reflected in the whole subscription - dashboard, web app results	iated web lication reports, API
Note: You will be able to change back the severity level of your findings at any time in the future.	
Cancel	ок

When the detection has been altered, the dialog will be refreshed to display an additional block notifying the user that the severity level for the detection has been either increased or decreased.

Vulnerability Details										
0	The s	everity le	Restore Standard Level							
	Update Update Date Comme	ed to level: ed by: ent	3 Hamza BENZ 06 May 2016	IOUCHE (quays_hb) 4:13PM GMT						
	Sever	ity Level ha	is been updated fo	r finding from 2 to 3. upo	lated					
URL: I	27(http://10.1	001 FTP use 0.26.238:80 647	ers with Blank Pas	sword Allowed	Web Application	Test WAS Application	Install Patch Ignore Fixe	d		
Patch Group OWAS WASC	# SP Base	- CWE - -	- CVSS Temporal	_	Authentication First Time Detected Last Time Detected Last Scan Date	Not Used 19 Nov 2009 6:30PM GMT 20 Nov 2009 7:31PM GMT 12 Nov 2012 9:42PM GMT				
Deta	ails				Times Detected	1 view history	Show			
Det	etection Information									
Parameter:		N	o param has been r	equired for detecting the	information.					

Enhanced Display for Severity Level Text with Severity Icon

The Qualys severity name for each finding used to not be displayed. A small graphic image indicated the severity. The severity level names are defined in the appendix, but the severity name (5, 4, 3, 2, 1 –Confirmed, Potential) was never visible. Now the severity name as part of the severity information is displayed next to the severity graphic.

WAS Sca	n Report			
15	0001 Reflected Cross-Site Scripting (XSS)	Vulnerabilities		
URL: https://1	0.10.26.238/?accountcorp=corporate			
Finding #	1398012(38632593)	Severity	Confirmed Vulnerability - Level 5	
Group	Cross-Site Scripting	First Time Detected	16 May 2016 02:54 GMT-0400	
CWE	<u>CWE-79</u>	Last Time Detected	16 May 2016 02:54 GMT-0400	
OWASP	A3 Cross-Site Scripting (XSS)	Last Time Tested	16 May 2016 02:54 GMT-0400	
WASC	WASC-8 Cross-Site Scripting	Times Detected	1	
CVSS Base	4.3 CVSS Temporal 3.9			

Enhanced Reporting Detail for Function

We previously introduced and started displaying Function with SOAP call fuzzing. Besides it's usefulness for ID calculation (to make different API calls unique) the element is now displayed in the UI for enhanced reporting detail.

15	0046 Reflec	cted Cross-Site Scrip	ting In HTTP Header		Install Patch Ignore
JRL: https://10	.10.26.238/	poq/aboutus.php			
Finding #	1409794	(Web Application	Copy of <script>alert()</script>
Patch #	-			Authentication	Not Used
Group	Cross-S	ite Scripting			
WE	CWE-79			First Time Detected	21 Oct 2015 12:30PM GMT
OWASP	A3 Cros	s-Site Scripting (XSS)		Last Time Detected	14 Dec 2015 12:30PM GMT
VASC	WASC-8	Cross-Site Scripting		Last Scan Date	15 Dec 2015 12:30PM GMT
		20 S. 10		Times Detected	7 View History
CVSS Base	4.3	CVSS Temporal	3.9	External References	22 NO
Details					Show
Detection	Informati	on			
Detection Parameter: Function: Access Path	Informati It TI W	ON has been detected by <u>he payloa</u> ds section v elcome ere is the path follow	exploiting the parameter vill display a list of tests that ed by the scanner to reach t	cookie2 show how the param cou he exploitable URL:	IId have been exploited to collect the information
Detection Parameter: Function: Access Path http://1 http://	Informati It N 1: H 0.10.26.2 10.10.26.	ON has been detected by he payloads section v elcome ere is the path follow 38/ 238/bog/parseAct.	exploiting the parameter ill display a list of tests that ed by the scanner to reach t .cn.php	cookie2 show how the param cou he exploitable URL:	IId have been exploited to collect the information
Detection Parameter: Punction: Access Path http://l http:// Payloads	Informati It TI W 0.10.26.2 (10.10.26.2 (3 instance	ON has been detected by he payloads section v elcome ere is the path follow 38/ 238/boq/parseAct. ES)	exploiting the parameter rill display a list of tests that ad by the scanner to reach t	cookie2 show how the param cou he exploitable URL:	IId have been exploited to collect the information Show all payloads

WAS Module Global Settings Support

This new feature now allows Locale settings, Scan settings and Report settings to be configurable at the customer level in order to allow editing the default global settings by the manager.

We have added a new tab panel, 'Defaults' under the "Reports" section to add defaults for report settings:



Report Settings - View Mode

Web Application Scanning	v	\geq	Help 🗸	Hamza BENZIOUCHE 🗸	Log Out
Dashboard Web Applica	tions Scans Burp Reports Configuration KnowledgeBase				
III Report Manageme	nt Reports Schedules Templates Defaults				
Edit Settings	Define report defaults values			Cancel	Save
Report >	Default Download Format				
	Specify a default format to be used when downloading report Extensible Markup Language (XML)				
	User Limit* You can update the quota allowed per user for storing reports. The limit per user cannot exceed the global limit set for the subscription (700 MB). 235 MB				
	Severity Levels Specify what type of severity levels shall be used for each finding.				
	IUF 5 (Urgent), 4 (Critical), 3 (Serious), 2 (Medium), 1 (Minimal) HIGH High (Severity levels 5 and 4), Medium (level 3) and Low (levels 2 and 1)				

Report Settings – Edit Mode

We added a new tab panel, 'Defaults' under "Scans" section to add defaults for scan settings:

Web Application Scanning	✓ Hetp ✓ Hamza BENZIOUCHE ✓ Log Out
Dashboard Web Applicat	ions Scans Burp Reports Configuration KnowledgeBase
Scan Management	Scan List Schedules Option Profiles Defaults
View Settings	Define scan defaults values Edit
Scans Edit >	Scan Auto Delete Limit 9 Scan Title Format Test title of
	Scan Settings (View Mode)
Dashboard Web Applicatio	ns Scans Burp Reports Configuration KnowledgeBase
Scan Management	Scan List Schedules Option Profiles Defaults
Edit Settings	Define scan defaults values Cancel Save
Scans >	Scan Auto Delete Limit *
	Number of months before scans are automatically deleted (max 12 months)
	Automatically delete scan results after 6 Month(s)
	Scan Title Format
	Default value of the scan title, you can use <type> or <date> to include respectively the type and the date of the scan in the title.</date></type>
	Web Application test 2 <type> - <date></date></type>
	Soon pattings Edit Made
	Scan settings - Eait Mode

We added a new tab panel, 'Defaults' under "Users" section in Admin module to add defaults for locale settings:

dmininistrator 🗸 🗸						Help 🗸	Hamza BENZIOUCHE 🗸	Log
rs Action Log								
_								
J User Management	User Management	Role Management	Defaults					
ew Settings	Define user defaults val	lues						Edit
cale >	Browser Time Zone GMT +02:00 CSV List Separator							
			I	Locale Settings (Vie	w Mode)			
dmininistrator 🗸			l	Locale Settings (Vie	w Mode)	Help 🗸	Hamza BENZIOUCHE 🛩	Log C
dmininistrator 🗸			I	Locale Settings (Vie	w Mode)	Help 🗸	Hamza BENZIOUCHE 🗸	Log O
dmininistrator v ers Action Log J User Management	User Management	Role Management	Defaults	Locale Settings (Vie	w Mode)	Help 🗸	Hanza BENZIOUCHE 🗸	Log C
tmininistrator v rs Action Log] User Management lit Settings	User Management Define user defaults val	Role Management	Defaults	Locale Settings (Vie	w Mode)	Help 🗸	Hamza BENZIOUCHE 🗸 Cancel	Log O Save
dmininistrator v ers Action Log User Management Jit Settings	User Management Define user defaults va Any dates daptayed on the user in	Role Management lues	Defaults if defined.	Locale Settings (Vie	w Mode)	Help 🗸	Hamza BENZIOUCHE 🗸 Cancel	Log C Save
dmininistrator v ers Action Log C User Management dit Settings scale	User Management Define user defaults val Any dates daptayed on the user in Use browser time zone	Role Management lues	Defaults if defined.	Locale Settings (Vie	w Mode)	☐ Нер ↓	Hamza BENZIOUCHE 🗸 Cancel	Log C Save
dmininistrator v ers Action Log C User Management dit Settings scale	User Management Define user defaults val Any dates daplayed on the user in Use browser time zone Use custom time zone	Role Management lues	Defaults If defined.	Locale Settings (Vie	w Mode)	Hep 🗸	Hamza BENZIOUCHE 🗸 Cancel	Log O
dmininistrator v ers Action Log User Management dit Settings occile	User Management Define user defaults val Any dates displayed on the user in Use browser time zone Use custom time zone CSV Luis Separator [*]	Role Management lues	Defaults If defined.	Locale Settings (Vie	w Mode)	∭ Нер ∨	Hamza BENZIOUCHE 🗸 Cancel	Log O Save
Idmininistrator v ers Action Log User Management dit Settings ocale	User Management Define user defaults val Any dates displayed on the user if Use browser time zone Use custom time zone CSV List Separator* Specify a user separator to be use	Role Management lues tterface will use user länezone, ed when exporting data list in c	Defaults If defined.	Locale Settings (Vie	w Mode)	∭ Нер ∨	Hamza BENZIOUCHE 🗸 Cancel	Log O
Idmininistrator v ers Action Log User Management dit Settings ocale	User Management Define user defaults val Any dates displayed on the user in Use browser time zone Use custom time zone CSV List Separator* Specty a user separator to be use ,	Role Management Iues Iterface will use user lämezone, ad when exporting data list in ca	Defaults If defined.	Locale Settings (Vie	w Mode)	Hep 🗸	Hamza BENZIOUCHE 🛩 Cancel	Log C
dmininistrator v ers Action Log User Management dit Settings ocale	User Management Define user defaults val Any dates displayed on the user is Use browser time zone Use custom time zone CSV List Separator* Specify a user separator to be use ,	Role Management lues Interface will use user länezone, ad when exporting data list in co	I defined.	Locale Settings (Vie	w Mode)	lep ↓	Hamza BENZIOUCHE v Cancel	Log O Save

Locale settings - Edit Mode